

105TH CONGRESS
1ST SESSION

H. R. 1903

To amend the National Institute of Standards and Technology Act to enhance the ability of the National Institute of Standards and Technology to improve computer security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 17, 1997

Mr. SENSENBRENNER (for himself, Mr. BROWN of California, Mrs. MORELLA, Mr. GORDON, Mr. DAVIS of Virginia, Ms. STABENOW, Mr. EHLERS, Ms. JACKSON-LEE of Texas, Mr. SESSIONS, Mr. PICKERING, Mr. TRAFICANT, Mr. COOK, and Mr. CANNON) introduced the following bill; which was referred to the Committee on Science

A BILL

To amend the National Institute of Standards and Technology Act to enhance the ability of the National Institute of Standards and Technology to improve computer security, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Computer Security
5 Enhancement Act of 1997”.

6 **SEC. 2. FINDINGS AND PURPOSES.**

7 (a) FINDINGS.—The Congress finds the following:

1 (1) The National Institute of Standards and
2 Technology has responsibility for developing stand-
3 ards and guidelines needed to ensure the cost-effec-
4 tive security and privacy of sensitive information in
5 Federal computer systems.

6 (2) The Federal Government has an important
7 role in ensuring the protection of sensitive, but un-
8 classified, information controlled by Federal agen-
9 cies.

10 (3) Technology that is based on the application
11 of cryptography exists and can be readily provided
12 by private sector companies to ensure the confiden-
13 tiality, authenticity, and integrity of information
14 associated with public and private activities.

15 (4) The development and use of encryption
16 technologies should be driven by market forces rath-
17 er than by Government imposed requirements.

18 (5) Federal policy for control of the export of
19 encryption technologies should be determined in
20 light of the public availability of comparable
21 encryption technologies outside of the United States
22 in order to avoid harming the competitiveness of
23 United States computer hardware and software com-
24 panies.

25 (b) PURPOSES.—The purposes of this Act are to—

1 (1) reinforce the role of the National Institute
2 of Standards and Technology in ensuring the secu-
3 rity of unclassified information in Federal computer
4 systems;

5 (2) promote technology solutions based on pri-
6 vate sector offerings to protect the security of Fed-
7 eral computer systems; and

8 (3) provide the assessment of the capabilities of
9 information security products incorporating cryptog-
10 raphy that are generally available outside the United
11 States.

12 **SEC. 3. VOLUNTARY STANDARDS FOR PUBLIC KEY MAN-**
13 **AGEMENT INFRASTRUCTURE.**

14 Section 20(b) of the National Institute of Standards
15 and Technology Act (15 U.S.C. 278g–3(b)) is amended—

16 (1) by redesignating paragraphs (2), (3), (4),
17 and (5) as paragraphs (3), (4), (7), and (8), respec-
18 tively; and

19 (2) by inserting after paragraph (1) the follow-
20 ing new paragraph:

21 “(2) upon request from the private sector, to
22 assist in establishing voluntary interoperable stand-
23 ards, guidelines, and associated methods and tech-
24 niques to facilitate and expedite the establishment of
25 non-Federal management infrastructures for public

1 keys that can be used to communicate with and con-
2 duct transactions with the Federal Government;”.

3 **SEC. 4. SECURITY OF FEDERAL COMPUTERS AND NET-**
4 **WORKS.**

5 Section 20(b) of the National Institute of Standards
6 and Technology Act (15 U.S.C. 278g–3(b)), as amended
7 by section 3 of this Act, is further amended by inserting
8 after paragraph (4), as so redesignated by section 3(1)
9 of this Act, the following new paragraphs:

10 “(5) to provide guidance and assistance to Fed-
11 eral agencies in the protection of interconnected
12 computer systems and to coordinate Federal re-
13 sponse efforts related to unauthorized access to Fed-
14 eral computer systems;

15 “(6) to perform evaluations and tests of—

16 “(A) information technologies to assess
17 security vulnerabilities; and

18 “(B) commercially available security prod-
19 ucts for their suitability for use by Federal
20 agencies for protecting sensitive information in
21 computer systems;”.

22 **SEC. 5. COMPUTER SECURITY IMPLEMENTATION.**

23 Section 20 of the National Institute of Standards and
24 Technology Act (15 U.S.C. 278g–3) is further amended—

1 (1) by redesignating subsections (c) and (d) as
2 subsections (f) and (g), respectively; and

3 (2) by inserting after subsection (b) the follow-
4 ing new subsection:

5 “(c) In carrying out subsection (a)(3), the Institute
6 shall—

7 “(1) emphasize the development of technology-
8 neutral policy guidelines for computer security prac-
9 tices by the Federal agencies;

10 “(2) actively promote the use of commercially
11 available products to provide for the security and
12 privacy of sensitive information in Federal computer
13 systems; and

14 “(3) participate in implementations of
15 encryption technologies in order to develop required
16 standards and guidelines for Federal computer sys-
17 tems, including assessing the desirability of and the
18 costs associated with establishing and managing key
19 recovery infrastructures for Federal Government in-
20 formation.”.

21 **SEC. 6. COMPUTER SECURITY REVIEW, PUBLIC MEETINGS,**
22 **AND INFORMATION.**

23 Section 20 of the National Institute of Standards and
24 Technology Act (15 U.S.C. 278g–3), as amended by this
25 Act, is further amended by inserting after subsection (c),

1 as added by section 5 of this Act, the following new sub-
2 section:

3 “(d)(1) The Institute shall solicit the recommenda-
4 tions of the Computer System Security and Privacy Advi-
5 sory Board, established by section 21, regarding standards
6 and guidelines that are being considered for submittal to
7 the Secretary of Commerce in accordance with subsection
8 (a)(4). No standards or guidelines shall be submitted to
9 the Secretary prior to the receipt by the Institute of the
10 Board’s written recommendations. The recommendations
11 of the Board shall accompany standards and guidelines
12 submitted to the Secretary.

13 “(2) There are authorized to be appropriated to the
14 Secretary of Commerce \$1,000,000 for fiscal year 1998
15 and \$1,030,000 for fiscal year 1999 to enable the Com-
16 puter System Security and Privacy Advisory Board, estab-
17 lished by section 21, to identify emerging issues related
18 to computer security, privacy, and cryptography and to
19 convene public meetings on those subjects, receive presen-
20 tations, and publish reports, digests, and summaries for
21 public distribution on those subjects.”.

22 **SEC. 7. EVALUATION OF CAPABILITIES OF FOREIGN**
23 **ENCRYPTION.**

24 Section 20 of the National Institute of Standards and
25 Technology Act (15 U.S.C. 278g–3), as amended by this

1 Act, is further amended by inserting after subsection (d),
2 as added by section 6 of this Act, the following new sub-
3 section:

4 “(e)(1) If the Secretary has imposed, or proposes to
5 impose, export restrictions on a product that incorporates
6 encryption technologies, the Institute may accept technical
7 evidence from the commercial provider of the product of-
8 fered to indicate that encryption technologies, embodied
9 in the form of software or hardware, that are offered and
10 generally available outside the United States for use, sale,
11 license, or transfer (whether for consideration or not) pro-
12 vide stronger participation for privacy of computer data
13 and transmissions of information in digital form than the
14 encryption technologies incorporated in the commercial
15 provider’s product.

16 “(2) Within 30 days after accepting technical evi-
17 dence from a commercial provider under paragraph (1),
18 the Institute shall evaluate the accuracy and completeness
19 of the technical evidence and transmit to the Secretary,
20 and to the Committee on Science of the House of Rep-
21 resentatives and the Committee on Commerce, Science,
22 and Transportation of the Senate, a report containing the
23 results of that evaluation. The Institute may obtain assist-
24 ance from other Federal and private sector entities in car-
25 rying out evaluations under this paragraph.

1 “(3) Not later than 180 days after the date of the
2 enactment of the Computer Security Enhancement Act of
3 1997, the Institute shall develop standard procedures and
4 tests for determining the capabilities of encryption tech-
5 nologies, and shall provide information regarding those
6 procedures and tests to the public.

7 “(4) The Institute may require a commercial provider
8 seeking evaluation under this subsection to follow proce-
9 dures and carry out tests developed by the Institute pursu-
10 ant to paragraph (3).”.

11 **SEC. 8. LIMITATION ON PARTICIPATION IN REQUIRING**
12 **ENCRYPTION STANDARDS.**

13 Section 20 of the National Institute of Standards and
14 Technology Act (15 U.S.C. 278g–3), as amended by this
15 Act, is further amended by adding at the end the following
16 new subsection:

17 “(h) The Institute shall not promulgate, enforce, or
18 otherwise adopt standards, or carry out activities or poli-
19 cies, for the Federal establishment of encryption standards
20 required for use in computer systems other than Federal
21 Government computer systems.”.

22 **SEC. 9. MISCELLANEOUS AMENDMENTS.**

23 Section 20 of the National Institute of Standards and
24 Technology Act (15 U.S.C. 278g–3), as amended by this
25 Act, is further amended—

1 (1) in subsection (b)(8), as so redesignated by
 2 section 3(1) of this Act, by inserting “to the extent
 3 that such coordination will improve computer secu-
 4 rity and to the extent necessary for improving such
 5 security for Federal computer systems” after “Man-
 6 agement and Budget)”;

7 (2) in subsection (f), as so redesignated by sec-
 8 tion 5(1) of this Act, by striking “shall draw upon”
 9 and inserting in lieu thereof “may draw upon”;

10 (3) in subsection (f)(2), as so redesignated by
 11 section 5(1) of this Act, by striking “(b)(5)” and in-
 12 serting in lieu thereof “(b)(5)”; and

13 (4) in subsection (g)(1)(B)(i), as so redesign-
 14 ated by section 5(1) of this Act, by inserting “and
 15 computer networks” after “computers”.

16 **SEC. 10. FEDERAL COMPUTER SYSTEM SECURITY TRAIN-**
 17 **ING.**

18 Section 5(b) of the Computer Security Act of 1987
 19 (49 U.S.C. 759 note) is amended—

20 (1) by striking “and” at the end of paragraph
 21 (1);

22 (2) by striking the period at the end of para-
 23 graph (2) and inserting in lieu thereof “; and”; and

24 (3) by adding at the end the following new
 25 paragraph:

1 “(3) to include emphasis on protecting sensitive
2 information in Federal databases and Federal com-
3 puter sites that are accessible through public net-
4 works.”.

5 **SEC. 11. COMPUTER SECURITY FELLOWSHIP PROGRAM.**

6 There are authorized to be appropriated to the Sec-
7 retary of Commerce \$250,000 for fiscal year 1998 and
8 \$250,000 for fiscal year 1999 for the Director of the Na-
9 tional Institute of Standards and Technology for fellow-
10 ships, subject to the provisions of section 18 of the Na-
11 tional Institute of Standards and Technology Act (15
12 U.S.C. 278g-1), to support students at institutions of
13 higher learning in computer security. Amounts authorized
14 by this section shall not be subject to the percentage limi-
15 tation stated in such section 18.

16 **SEC. 12. STUDY OF PUBLIC KEY INFRASTRUCTURE BY THE**
17 **NATIONAL RESEARCH COUNCIL.**

18 (a) REVIEW BY NATIONAL RESEARCH COUNCIL.—
19 Not later than 90 days after the date of the enactment
20 of this Act, the Secretary of Commerce shall enter into
21 a contract with the National Research Council of the Na-
22 tional Academy of Sciences to conduct a study of public
23 key infrastructures for use by individuals, businesses, and
24 government.

1 (b) CONTENTS.—The study referred to in subsection

2 (a) shall—

3 (1) assess technology needed to support public
4 key infrastructures;

5 (2) assess current public and private plans for
6 the deployment of public key infrastructures;

7 (3) assess interoperability, scalability, and in-
8 tegrity of private and public entities that are ele-
9 ments of public key infrastructures;

10 (4) make recommendations for Federal legisla-
11 tion and other Federal actions required to ensure
12 the national feasibility and utility of public key in-
13 frastructures; and

14 (5) address such other matters as the National
15 Research Council considers relevant to the issues of
16 public key infrastructure.

17 (c) INTERAGENCY COOPERATION WITH STUDY.—All
18 agencies of the Federal Government shall cooperate fully
19 with the National Research Council in its activities in car-
20 rying out the study under this section, including access
21 by properly cleared individuals to classified information if
22 necessary.

23 (d) REPORT.—Not later than 18 months after the
24 date of the enactment of this Act, the Secretary of Com-
25 merce shall transmit to the Committee on Science of the

1 House of Representatives and the Committee on Com-
2 merce, Science, and Transportation of the Senate a report
3 setting forth the findings, conclusions, and recommenda-
4 tions of the National Research Council for public policy
5 related to public key infrastructures for use by individuals,
6 businesses, and government. Such report shall be submit-
7 ted in unclassified form.

8 (e) AUTHORIZATION OF APPROPRIATIONS.—There
9 are authorized to be appropriated to the Secretary of Com-
10 merce \$450,000 for fiscal year 1998, to remain available
11 until expended, for carrying out this section.

12 **SEC. 13. SOURCE OF AUTHORIZATIONS.**

13 Amounts authorized to be appropriated by this Act
14 shall be derived from amounts authorized under the Na-
15 tional Institute of Standards and Technology Authoriza-
16 tion Act of 1997.

